UNITED STATES DISTRICT COURT
FOR THE
DISTRICT OF VERMONT

SHAWNA GABORIAULT, on behalf of herself and all others similarly situated, Plaintiff, v. PRIMMER, PIPER, EGGLESTON, & CRAMER, P.C., AND JOHN DOES 1 TO 10, Defendants.	)	Case No. 2:24-cv-113

OPINION AND ORDER

Plaintiff Shawna Gaboriault ("Plaintiff"), individually and as personal representative of a putative class, brings this action against the law firm of Primmer Piper Eggleston & Cramer and various John Does (collectively "PPEC") claiming that PPEC failed to protect her personal information from a cyberattack. Plaintiff specifically alleges that PPEC, while representing an opposing party in litigation, obtained her identity and health information and is now liable for damages resulting from the release of that information to an unknown third party.

Pending before the Court is PPEC's motion to dismiss pursuant Federal Rules of Civil Procedure 12(b)(1), 12(b)(6), and 12(f). PPEC first argues that Plaintiff lacks standing to sue because her damages claims are insufficient. PPEC also contends that Plaintiff has failed to state a plausible cause of

action because, among other things, PPEC owed her no duty, had no contractual obligations, and did not engage in any intentional conduct. Finally, PPEC moves to strike the class allegations, arguing that the damages claims are too divergent and non-specific to qualify for class certification. For the reasons set forth below, the motion to dismiss is granted in part and denied in part.

Factual Background

This case centers on a data breach that allegedly occurred between November 8 and November 11, 2021. On November 23, 2021, PPEC reported the breach to the Attorney General for the State of New Hampshire. The report stated that 265 New Hampshire residents were impacted, and that the information at issue may have included "names, Social Security numbers, driver's license numbers, financial account numbers, dates of birth, medical information, health insurance numbers, online credentials, tax identification numbers, passport numbers and/or electronic signatures." ECF No. 1 at 1, ¶ 1. PPEC also allegedly notified the Attorney General for the State of Maine, where five people were impacted by the data breach. The Complaint alleges that there are a total of 373 putative class members.

Plaintiff is a resident of Hardwick, Vermont. PPEC previously obtained her Protected Health Information ("PHI") and Personal Identifying Information ("PII") during the pendency of

a state court personal injury matter captioned *Shawna Gaboriault v. Eric Gilbertson*, 412-8-19 Wncv. PPEC represented the defendant in that case, Eric Gilbertson. The PHI and PII was allegedly exchanged during the normal course of litigation.

On August 4, 2022, PPEC sent a Notice of Security Incident ("NSI") to Plaintiff's attorney. The NSI provided the following information about the data breach:

> In November 2021, an unauthorized third party gained access to our network and copied a limited amount of data to an external data hosting site. We worked with the hosting site to lock down access to the account and delete the data. We have no reason to believe that any personal or confidential information has been disseminated or misused for the purpose of committing fraud or identity theft. We do not know the identity of the individual or individuals responsible for this incident. We are providing you with notice out of an abundance of caution as confidential information was placed at risk. A description of the attack and our response follows. The attack occurred in November of 2021. Malware was placed on [PPEC's] system through a bogus email link.
>
> A set of documents equaling approximately 76 GBs in size was identified for copying to a server in New Zealand. When the copying was discovered and stopped, 46 GBs of data had been copied. The server host terminated all access to the data. During the course of the download and prior to its stoppage, data that had been downloaded was potentially accessible.

Id. at 2-3, ¶ 4. The private information potentially exposed in the breach may have included Plaintiff's "Diagnosis/Clinical information, Doctor name or Practice Type, Medical History, Medical procedure information, Medical Record Number (MRN), Patient Name, Test results or lab reports, Treatment Type or

Location" and "Date of Birth (DOB)." *Id.* at 2, ¶ 3. The NSI stated that "we are not aware of any instances of dissemination, fraud or identity theft that have occurred as a result of the incident," "we are not aware of any access to the data," and that "the attack was deemed a failure." ECF No. 1-1 at 1.

Plaintiff now claims that PPEC's management of her PHI and PII was inadequate and negligent. Specifically, she claims that PPEC failed to implement and maintain reasonable security procedures and practices, and failed to ensure that its employees were properly trained. The Complaint claims a wide range of harms, including: reputational harm after publication of private facts from medical records; potential fraud and identity theft; untimely and inadequate notification of the data breach; out-of-pocket expenses and costs associated with the prevention, detection, recovery, and remediation from identity theft or fraud; lost opportunity costs and lost wages associated with the time and effort expended to mitigate the actual and future consequences of the breach; deprivation of the value of the class members' PII and PHI, for which there is allegedly a well-established national and international market; loss of the opportunity to control how the PII is used; and the continuing compromise and publication of PII.

Plaintiff initiated this case on February 2, 2024. The Complaint asserts causes of action for negligence; negligent

hiring and retention; breach of contract; breach of implied contract; invasion of privacy; publication of private facts; and unjust enrichment. The Complaint also claims that it meets the requirements for bringing a class action. For relief, the Complaint seeks both equitable relief and damages, including punitive damages.

PPEC now moves to dismiss pursuant Federal Rule of Civil Procedure 12(b)(1) for lack of Article III standing, arguing that Plaintiff's damages claims are insufficient. PPEC also asserts that the Complaint fails to explain how the alleged damages are fairly traceable to the cyberattack. PPEC further moves to dismiss pursuant to Fed. R. Civ. P. 12(b)(6), arguing that no common law duty existed to support negligence claims; that there was no contract to support Plaintiff's contract claims; that the Complaint alleges no intentional conduct to support invasion of privacy and publication of private information claims; and that Plaintiff's unjust enrichment claim is precluded (1) by her claims for monetary damages, and (2) because PPEC received no direct benefit from Plaintiff's information. Finally, PPEC moves pursuant to Fed. R. Civ. P. 12(f) to the strike class allegations for failure to satisfy the requirements of Fed. R. Civ. P. 23(a) and (b). In support of this final argument, PPEC argues that the lack of damages, and the divergence of damages, is fatal to class certification.

Discussion

I. Standing

PPEC first moves to dismiss the Complaint under Rule 12(b)(1) for lack of standing. To satisfy the constitutional requirements of Article III standing, "a plaintiff must demonstrate (1) that he or she suffered an injury in fact that is concrete, particularized, and actual or imminent, (2) that the injury was caused by the defendant, and (3) that the injury would likely be redressed by the requested judicial relief." *Thole v. U.S. Bank*, 590 U.S. 538, 540 (2020). A plaintiff has class standing if she plausibly alleges that she has personally suffered an actual injury as a result of the defendant's conduct, and that such conduct implicates the same concerns as that alleged to have caused injury to other members of the putative class by the same defendant. *NECA-IBEW Health & Welfare Fund v. Goldman Sachs & Co.*, 693 F.3d 145, 162 (2d Cir. 2012).

PPEC's first standing argument is that the Complaint does not allege a concrete injury in fact. PPEC notes that its NSI only gave notice of the possibility of data dissemination, and that the Complaint does not allege actual disclosure to, or misuse by, third parties. PPEC argues that the mere risk of future harm is not a concrete injury, that mitigation expenses are only recoverable if there is a substantial risk of future

harm, and that other non-specific claims such as lost time and diminution in value do not establish injury in fact.

The question of concrete injury is controlled by the Supreme Court's ruling in *TransUnion v. Ramirez*, 594 U.S. 413 (2021). *See Bohnak v. Marsh & McLennan Companies, Inc.*, 79 F.4th 276 (2d Cir. 2023). *TransUnion* recognized that concrete harm may be intangible, particularly where it bears a "close relationship to harms traditionally recognized as providing a basis for lawsuits in American courts. Those include, for example, reputational harms, disclosure of private information, and intrusion upon seclusion." 594 U.S. at 425. The Second Circuit observed in *Bohnak* that, "[s]ignificantly, the [*TransUnion*] Court concluded that the publication of false information ... was itself enough to establish a concrete injury; it did not take further steps to evaluate whether those third parties *used* the information in ways that harmed the class members." 79 F.4th at 284-85.

Bohnak applied *TransUnion* in a class action alleging release of the representative plaintiff's name and social security number to an unauthorized third party. 79 F.4th at 281. The court found that, as in *TransUnion*, "the core injury here – exposure of Bohnak's private PII to unauthorized third parties – bears some relationship to a well-established common-law analog: public disclosure of private facts." *Id.* at 285.

The court further concluded that such core injury "falls squarely within the scope of an intangible harm the Supreme Court has recognized [in *TransUnion*] as concrete." *Id.* at 286.

Following on *TransUnion*'s discussion of separate, concrete harms, *Bohnak* next found that the plaintiff had suffered such harms "as a result of the risk of future harm occasioned by the exposure of her PII." *Id.* *Bohnak* specifically cited the plaintiff's allegations of "'out-of-pocket expenses associated with the prevention, detection, and recovery from identify theft,' and 'lost time' and other 'opportunity costs' associated with attempting to mitigate the consequences of the data breach." *Id.* The court held that "[t]hese separate and concrete harms foreseeably arising from the exposure of Bohnak's PII to a malign outside actor, giving rise to a material risk of future harm, independently support standing." *Id.*

The allegations in this case largely mirror those that gave rise to standing in *Bohnak*. Here, Plaintiff alleges the disclosure of private information, which both the Supreme Court and Second Circuit have recognized as a concrete injury. *See TransUnion*, 594 U.S. at 432; *Bohnak*, 79 F.4th at 286. Plaintiff also claims separate harms such as mitigation costs, lost time, and diminution in value. *Bohnak* held that such claims support standing. 79 F.4th at 286.

Bohnak also explained, however, that finding a concrete injury "does not fully resolve the standing question because it addresses only one component of injury in fact." *Id.* at 287. The plaintiff also needed to establish that the injury was actual or imminent. *Id.* For that analysis, the Second Circuit followed *McMorris v. Carlos Lopez & Assocs., LLC*, 995 F.3d 295 (2d Cir. 2021), which set forth "three non-exhaustive factors" that bear on whether a data breach injury is actual or imminent: (1) "whether the data was compromised as the result of a targeted attack intended to get" PII; (2) whether "some part of the compromised dataset has been misused — even if a plaintiff's own data has not"; and (3) "whether the exposed PII is of the type 'more or less likely to subject plaintiffs to a perpetual risk of identity theft or fraud once it has been exposed.'" *Bohnak*, 79 F.4th at 288 (quoting *McMorris*, 995 F.3d at 301–03).

McMorris identified the first factor – whether the data was compromised as the result of a targeted attack – as the most important. 995 F.3d at 301. "[W]here plaintiffs demonstrate that a malicious third party intentionally targeted a defendant's system and stole plaintiffs' data stored on that system, courts have been more willing to find that those plaintiffs have established a likelihood of future identity theft or fraud sufficient to confer standing." *Id.* *McMorris* endorsed the Seventh Circuit's reasoning on this point: "Why

else would hackers break into a store's database and steal consumers' private information? Presumably, the purpose of the hack is, sooner or later, to make fraudulent charges or assume those consumers' identities." *Id.* (quoting *Remijas v. Neiman Marcus Grp., LLC*, 794 F.3d 688, 693 (7th Cir. 2015)).

Here, the Complaint alleges a targeted attack on PPEC's network. The NSI from PPEC revealed that "an unauthorized third party gained access to our network and copied a limited amount of data to an external hosting site.... Malware was placed on [PPEC's] system through a bogus email link." Documents were copied to a server in New Zealand, and the identity of "the person or persons responsible for this incident" was unknown. Those allegations support Plaintiff's claim that her information is likely to result in future identity theft or fraud since, as *Remijas* and *McMorris* both observed, such theft or fraud was presumably the ultimate purpose of the attack.

McMorris allowed that the second factor – whether some part of the data has been misused – is "not a necessary component of establishing standing." 995 F.3d at 301. Indeed, *Bohnak* found standing without any evidence of actual misuse. 79 F.4th at 289. In this case, the Complaint offers no allegation that the data of either the Plaintiff or any potential class members has been actually misused.

The third *McMorris* factor weighs in Plaintiff's favor. The Complaint alleges that the theft of PHI can result in insurance fraud and, for victims, the payment of "out-of-pocket costs for healthcare they did not receive in order to restore coverage." ECF No. 1 at 7-8, ¶ 28. The Complaint also alleges that PII can be used to conduct "synthetic identity theft" whereby a thief creates a new identity by combining the PII of one person with the Social Security number of another. *Id.* at 8-9, ¶ 31. The Court notes that this sort of "synthetic" theft does not require use of the Plaintiff's own Social Security number, as her identifying information can be merged with that of someone else to create a false identity. The Court therefore finds that the allegations of a targeted attack by an unauthorized party are "sufficient to suggest a substantial likelihood of future harm, satisfying the 'actual or imminent' harm" component of an injury in fact." *Bohnak*, 79 F.4th at 289; *see also In re Unite Here Data Sec. Incident Litig.*, No. 24-CV-1565(JSR), 2024 WL 3413942, at *3 (S.D.N.Y. July 15, 2024) (finding support for standing where plaintiffs asserted "allegations of theft of sensitive health information, which the complaint alleges is substantially more valuable to criminals than personally identifiable information").

In addition to injury in fact, a plaintiff must allege that the injury was caused by the actions of the defendant. In the

standing context, causation requires "a fairly traceable connection between the alleged injury in fact and the alleged conduct of the defendant." *Sprint Commc'ns Co., L.P. v. APCC Servs., Inc.*, 554 U.S. 269, 273 (2008) (cleaned up). PPEC argues that the Plaintiff has failed to establish traceability because her only claim is that the breach occurred. ECF No. 16 at 27. Plaintiff also claims, however, that the breach occurred as the result of PPEC's action or inaction.

The causal connection element of Article III standing "does not create an onerous standard. For example, it is a standard lower than that of proximate causation." *Carter v. HealthPort Techs., LLC*, 822 F.3d 47, 55 (2d Cir. 2016); *see also In re Unite Here Data Sec. Incident Litig.*, 2024 WL 3413942, at *4 ("Traceability is a lower bar than proving causation on the merits."). "The traceability requirement focuses on whether the asserted injury could have been a consequence of the actions of the defendant[.]" *Chevron Corp. v. Donziger*, 833 F.3d 74, 121 (2d Cir. 2016). "A defendant's conduct that injures a plaintiff but does so only indirectly, after intervening conduct by another person, may suffice for Article III standing." *Carter*, 822 F.3d at 55–56.

Here, the primary cause of the injury is the cyberattack itself. The alleged intervening conduct, however, was PPEC's failure to properly secure and protect the data. The Court

finds that the allegations of security failures brought against PPEC are sufficient to meet the causation requirement for standing. *See, e.g., In re U.S. Off. of Pers. Mgmt. Data Sec. Breach Litig.*, 928 F.3d 42, 49 (D.C. Cir. 2019) (concluding that plaintiffs' allegation of inadequate cybersecurity practices met the "'relatively modest' burden of alleging that their risk of future identity theft is fairly traceable to [defendants'] challenged conduct")(quoting *Bennett v. Spear*, 520 U.S. 154, 171 (1997)); *In re Canon U.S.A. Data Breach Litig.*, No. 20-CV-6239 (AMD) (SJB), 2022 WL 22248656, at *5 (E.D.N.Y. Mar. 15, 2022) ("The plaintiffs adequately allege that the injuries they suffered are 'fairly traceable' to Canon's 'inadequate information security practices' in collecting and storing employees' PII.").

The third prong of the standing test asks whether the injury will be redressed by a favorable decision. *Thole*, 590 U.S. at 540. Here, if the Plaintiff and the putative class are successful, the Court will be able to redress their alleged injuries by awarding damages for, among other things, the reasonable costs of mitigating or avoiding future identity theft. *See McFarlane v. Altice USA, Inc.*, 524 F. Supp. 3d 264, 273 (S.D.N.Y. 2021). In sum, Plaintiff has met her burden of showing a concrete injury in fact that is actual or imminent, is fairly traceable to PPEC's alleged actions, and can be redressed

by a favorable decision. Consequently, Plaintiff has established Article III standing.

II. Failure to State a Claim

PPEC next moves to dismiss pursuant to Federal Rule of Civil Procedure 12(b)(6), arguing that Plaintiff has failed to state a claim upon which relief can be granted. To survive a motion to dismiss for failure to state a claim, "a complaint must contain sufficient factual matter, accepted as true, to 'state a claim to relief that is plausible on its face.'" *Ashcroft v. Iqbal*, 556 U.S. 662, 678 (2009) (quoting *Bell Atl. Corp. v. Twombly*, 550 U.S. 544, 570 (2007)). "A claim has facial plausibility when the plaintiff pleads factual content that allows the court to draw the reasonable inference that the defendant is liable for the misconduct alleged." *Id.*

The plausibility standard requires "more than a sheer possibility that a defendant has acted unlawfully." *Id.* When assessing a complaint, courts draw all reasonable inferences in favor of the non-movant. *See In re Elevator Antitrust Litigation*, 502 F.3d 47, 50 (2d Cir. 2007). The Court is not bound to accept "legal conclusion[s] couched as [ ] factual allegation[s]" as true. *Drimal v. Tai*, 786 F.3d 219, 223 (2d Cir. 2015) (internal quotation omitted). It examines only the well-pleaded factual allegations "and then determine[s]

whether they plausibly give rise to an entitlement to relief." *Iqbal*, 556 U.S. at 679.

A. General Negligence

The first cause of action in the Complaint is a negligence claim. Under Vermont law, a claim for negligence has four elements: "a legal duty owed by defendant to plaintiff, a breach of that duty, actual injury to the plaintiff, and a causal link between the breach and the injury." *Stopford v. Milton Town Sch. Dist.*, 2018 VT 120, ¶ 12. PPEC moves to dismiss Plaintiff's negligence claim, arguing that it owed her no legal duty, that a criminal cyberattack was not reasonably foreseeable, and that Plaintiff's damages are insufficient and barred by the economic loss rule.

The Complaint alleges that PPEC owed a duty to Plaintiff and class members to exercise reasonable care to secure and safeguard their PII and PHI. ECF No. 1 at 18, ¶ 72. The Complaint also alleges that PPEC "knowingly disregard[ed] standard information security principles." *Id.* at 19, ¶ 79. Several courts have held that when an entity such as an employer or a retail business takes possession of PII and/or PHI, that entity owes a duty of reasonable care to safeguard the information. *See, e.g., Toretto v. Donnelley Fin. Sols., Inc.*, 583 F. Supp. 3d 570, 593 (S.D.N.Y. 2022) (concluding that company owed customers "a duty to exercise reasonable care

safeguarding their personal information"); *In re GE/CBPS Data Breach Litig.*, 2021 WL 3406374, at *8 (S.D.N.Y. Aug. 4, 2021) (concluding that employer owed employees "a duty to exercise reasonable care in safeguarding their PII"); *Sackin v. TransPerfect Glob., Inc.*, 278 F. Supp. 3d 739, 748 (S.D.N.Y. 2017) ("[E]mployers have a duty to take reasonable precautions to protect the PII that they require from employees."). Indeed, given the sensitive nature of such information, common sense dictates that someone in possession of another person's PII or PHI must take reasonably protective precautions. *See In re Sony Gaming Networks & Customer Data Sec. Breach Litig.*, 996 F. Supp. 2d 942, 966 (S.D. Cal. 2014) ("the Court finds the legal duty [to protect commercial consumer information] well supported by both common sense and California and Massachusetts law"); *Purvis v. Aveanna Healthcare, LLC*, 563 F. Supp. 3d 1360, 1370 (N.D. Ga. 2021) ("It also follows as a matter of common sense that, when patients and employees are required to turn over PII and PHI as a condition of medical care and employment, the entity receiving that information has some baseline obligation to adopt reasonable precautions to guard against known or reasonably foreseeable threats to the security of that information.").

PPEC contends that, under Vermont law, there is no duty to protect another from the actions of a third party absent a "special relationship" such as master-servant or parent-minor

child. In the data breach context, "affirmative conduct associated with an increased risk of harm can yield a special relationship for tort purposes." *In re Rutter's Inc. Data Sec. Breach Litig.*, 511 F. Supp. 3d 514, 529 (M.D. Pa. 2021); *see also* Jay P. Kesan & Carol M. Hayes, *Liability for Data Injuries*, 2019 U. Ill. L. Rev. 295, 321 (2019) ("A defendant who assumes custody or assumes responsibility of something may be held to have a special relationship with the plaintiff."). Here, PPEC affirmatively requested personal information on behalf of its client, and in doing so plausibly created a special relationship. That relationship gave rise to a duty to reasonably protect Plaintiff's information from harm.

With respect to foreseeability, the Complaint alleges that by knowingly disregarding "obvious risks, and by allowing unmonitored and unrestricted access to unsecured Private Information," PPEC failed to protect against "the known risk and foreseeable likelihood of breach and misuse." ECF No. 1 at 19, ¶ 79. The Vermont Supreme Court has noted that the "question of foreseeability is ordinarily a heavily fact-based determination." *Blondin v. Milton Town Sch. Dist.*, 2021 VT 2, ¶ 55 n.6. As the Court must accept the factual claims in the Complaint as true, it finds that allegations of knowingly disregarding an obvious harm are sufficient. *See also, e.g., Haney v. Charter Foods N., LLC*, No. 2:23-CV-168, 2024 WL

4054361, at *9 (E.D. Tenn. Aug. 28, 2024) ("Given the high level of foreseeability and known risks of data breaches, Defendants had a duty to take reasonable care to protect Plaintiffs from the data breach.").

PPEC's final argument with respect to general negligence is that Plaintiff has failed to allege sufficient damages. For support, PPEC relies in part on its injury-in-fact analysis regarding standing. The Court found in Plaintiff's favor on that issue and does so again here. *Cf. Bohnak*, 79 F.4th at 286 (finding "separate and concrete harms foreseeably arising from the exposure of Bohnak's PII to a malign outside actor").

PPEC also argues that Plaintiff's negligence damages are barred by the economic loss rule. "In its most general sense, with certain exceptions, the economic-loss rule prohibits recovery in tort for purely economic losses." *Sutton v. Vermont Reg'l Ctr.*, 2019 VT 71A, ¶ 30. One exception recognized by the Vermont Supreme Court is where there is "a special relationship between the alleged tortfeasor and the individual who sustains purely economic damages sufficient to compel the conclusion that the tortfeasor had a duty to the particular plaintiff and that the injury complained of was clearly foreseeable to the tortfeasor." *Springfield Hydroelectric Co. v. Copp*, 172 Vt. 311, 316 (2001) (quotation omitted). As discussed above, and accepting the allegations set forth in the Complaint as true,

Plaintiff has alleged sufficient facts to support her claim to a special relationship, and that her damages were foreseeable. Accordingly, the Court finds that, at this stage in the case, the economic loss rule does not bar Plaintiff's claims. *See also, e.g., Toretto*, 583 F. Supp. 3d at 590 (concluding that, under New York law, economic loss doctrine did not bar the plaintiff's negligence claim in a data breach case); *In re Cap. One Consumer Data Sec. Breach Litig.*, 488 F. Supp. 3d 374, 401 (E.D. Va. 2020) ("Plaintiffs have alleged facts that make plausible negligence claims [regarding a data breach] under Virginia law that would not be barred under the economic loss rule."). The motion to dismiss Plaintiff's general negligence claim is therefore denied.

B. Negligent Hiring and Retention

Count Two of the Complaint alleges negligent hiring and retention. Specifically, the Complaint claims that "Defendants failed to exercise reasonable care in its/their hiring and retention practices to discover whether their employees, independent contractors and/or third-party vendors were unfit, incompetent, unable, or unwilling to employ adequate security measures." ECF No. 1 at 21, ¶ 88. PPEC argues that this claim is too conclusory to withstand a motion to dismiss, as it relies purely on the fact that the data breach occurred

without any specifics about flaws in hiring or retention practices.

The Court agrees that the allegations in the Complaint are conclusory, as they provide no factual basis for claiming that PPEC's hiring and/or retention was negligent. "While a complaint attacked by a Rule 12(b)(6) motion to dismiss does not need detailed factual allegations, a plaintiff's obligation to provide the 'grounds' of his 'entitle[ment] to relief' requires more than labels and conclusions, and a formulaic recitation of the elements of a cause of action will not do." *Twombly*, 550 U.S. at 555 (quoting Fed. R. Civ. P. 8(a)(2)). "[T]he tenet that a court must accept as true all of the allegations contained in a complaint is inapplicable to ... [t]hreadbare recitals of the elements of a cause of action, supported by mere conclusory statements." *Iqbal*, 556 U.S. at 678.

Plaintiff argues that because a PPEC employee apparently opened an email attachment that allowed attached malware to take effect, there must have been inadequate training and/or hiring of personnel. This factual assertion says little about PPEC's information technology hiring or retention practices, and whether those practices were sufficient to safeguard Plaintiff's PII and PHI from a criminal cyberattack. The claim of negligent hiring and/or retention is therefore dismissed without prejudice. *See, e.g., Cruz v. New York*, 24 F. Supp. 3d 299,

311–12 (W.D.N.Y. 2014) (finding that dismissal under Rule 12(b)(6) was warranted where the plaintiff's claims of negligent hiring, training, and retention were "conclusory and unsupported by any factual allegations supporting his assertion"); *Ross v. Mitsui Fudosan, Inc.*, 2 F. Supp. 2d 522, 532–33 (S.D.N.Y. 1998) ("Conclusory allegations of negligent supervision are insufficient to overcome a motion to dismiss.").

C. Breach of Contract

PPEC next moves to dismiss Plaintiff's breach of contract claim, arguing that there was never a contract between the parties. Plaintiff's briefing does not address that portion of the motion to dismiss, and the Complaint alleges only that members of the proposed class may have had contracts with PPEC. "It is well established that 'a plaintiff must demonstrate standing for each claim [s]he seeks to press.'" *Mahon v. Ticor Title Ins. Co.*, 683 F.3d 59, 64 (2d Cir. 2012) (quoting *DaimlerChrysler Corp. v. Cuno*, 547 U.S. 332, 335 (2006)). Because Plaintiff cannot move forward with the breach of contract claim herself, that claim is dismissed without prejudice.

D. Breach of Implied Contract

Count Four of the Complaint alleges that PPEC required Plaintiff and the proposed class members to share their personal information, and in doing so created an implied agreement that

the information would be kept secure. The Complaint also alleges that PPEC received a benefit as a result of this agreement. PPEC's motion to dismiss argues that the only benefit was received by its client, Mr. Gilbertson.

Vermont law recognizes that a meeting of the minds to enter into an unexpressed agreement can constitute an implied contract in fact. *Morse v. Kenney*, 87 Vt. 445 (1914).[1] "An implied-in-fact contract thus requires a mutual intent to contract." *Retail Pipeline, LLC*, 557 F. Supp. 3d at 554 (quotation omitted). The concept of an implied promise in the context of a data breach has been endorsed by at least one other court in this Circuit:

> Plaintiffs allege that when they provided their private information to Freestyle (as required to purchase from ShopRuger), Freestyle made the implied promise that the information would be protected and kept secure from further disclosure. With the data breach, Freestyle allegedly broke this promise. With these allegations, the Court concludes that Plaintiffs have plausibly alleged an implied contract with Freestyle as well as a breach of that implied contract.

[1] Vermont also recognizes an implied contract in law, which "is another term for unjust enrichment." *Retail Pipeline, LLC v. Blue Yonder Grp., Inc.*, 557 F. Supp. 3d 535, 554 (D. Vt. 2021), *aff'd sub nom. Retail Pipeline, LLC v. Blue Yonder, Inc.*, No. 21-2401-CV, 2022 WL 17660545 (2d Cir. Dec. 14, 2022). Because Plaintiff alleges unjust enrichment in a separate cause of action, and PPEC has moved to dismiss that cause of action, the Court will address that claim below.

Jones v. Sturm, Ruger & Co., Inc., No. 3:22-CV-1233 (KAD), 2024 WL 1307148, at *9 (D. Conn. Mar. 27, 2024). Another court recently reasoned that "it is difficult to imagine how, in our day and age of data and identity theft, the mandatory receipt of Social Security numbers or other sensitive personal information would not imply the recipient's assent to protect the information sufficiently." *Attias v. CareFirst, Inc.*, No. 15-CV-882 (CRC), 2023 WL 5952052, at *6 (D.D.C. Sept. 13, 2023) (quoting *Castillo v. Seagate Tech., LLC*, No. 16-CV-01958 (RS), 2016 WL 9280242, at *9 (N.D. Cal. Sept. 14, 2016)); *see also Anderson v. Hannaford Bros. Co.*, 659 F.3d 151, 159 (1st Cir. 2011) ("a jury could reasonably find an implied contract between Hannaford and its customers that Hannaford ... would take reasonable measures to protect the information").

The Vermont Supreme Court has not addressed the question of implied contracts in the data breach context. This Court has previously determined that to prevail on an implied-in-fact contract claim under Vermont law, "a plaintiff must demonstrate mutual intent to contract and acceptance of the offer." *Mount Snow Ltd. v. ALLI, the All. of Action Sports*, No. 1:12-CV-22-JGM, 2013 WL 4498816, at *8 (D. Vt. Aug. 21, 2013). The Complaint in this case alleges that a promise of safekeeping was implied when PPEC took possession of Plaintiff's sensitive information, and that Plaintiff provided her information in

exchange for that promise. These facts, accepted as true, state a plausible claim of mutual offer and acceptance. *See, e.g., Keown v. Intn'l Assoc. of Sheet Metal Air Rail Transp. Workers*, No. 23-CV-3570 (CRC), 2024 WL 4239936, at *13 (D.D.C. Sept. 19, 2024) ("The Court then joins numerous other courts in concluding that an obligation to reasonably safeguard the [plaintiffs'] PII from unauthorized access or disclosure is sufficiently definite to support an implied contract.) (quotations omitted)).

While PPEC contends that it received no benefit from the personal information, the Court finds this argument unpersuasive since acquisition of the PII and PHI afforded at least a joint benefit to Mr. Gilbertson and his attorneys. In any civil litigation, the interests of the attorney and his or her client are necessarily intertwined to the extent that success is beneficial to both. Accordingly, information that may lead to such success offers a benefit not just to the client, but also to the firm. The motion to dismiss the implied contract claim is therefore denied.

E. Invasion of Privacy

PPEC next moves to dismiss Plaintiff's invasion of privacy claim, arguing that the Complaint fails to allege either substantial or intentional conduct. In Vermont, "[i]nvasion of privacy is a substantial, intentional intrusion upon the solitude or seclusion of another, or upon his private affairs or

concerns, which would be highly offensive to a reasonable person." *Harris v. Carbonneau*, 165 Vt. 433, 439 (1996) (citing *Hodgdon v. Mount Mansfield Co.*, 160 Vt. 150, 162 (1992); Restatement (Second) of Torts §§ 652A, 652B (1977)). PPEC argues that the Complaint fails to state an invasion of privacy claim because there is no allegation of substantial, intentional conduct.

The Court agrees. The Complaint alleges that "Defendant's failure to safeguard and protect Plaintiff and Class Members' PII/PHI was a direct and proximate cause of an unauthorized third party accessing and obtaining Plaintiff and Class Members' PII/PHI as a matter of law." ECF No. 1 at 25, ¶ 115. There is no allegation of intentional invasion into private affairs.

The cases cited by Plaintiff in opposition to the motion to dismiss are distinguishable. Plaintiff relies in part upon *Dasler v. Knapp*, in which the plaintiff brought an intrusion upon seclusion claim against his ex-wife for allegedly using his computer to intercept, read, and delete emails, and placed a tracking device on their child to monitor where plaintiff went with the child during visitation. No. 2:21-CV-135, 2021 WL 4134398, at *6 (D. Vt. Sept. 10, 2021). Plaintiff also cites *Nashef v. AADCO Med., Inc.*, in which the plaintiff's co-worker "surreptitiously accessed his password-protected email account and sent emails purporting to be from" the plaintiff. No. 5:12-

CV-243, 2013 WL 12347190, at *6 (D. Vt. Apr. 29, 2013). Both *Dasler* and *Nashef* involved intentional actions to intrude upon alleged areas of privacy.

This case presents no such intentional conduct. In opposition to the motion to dismiss, Plaintiff submits that an allegation of reckless disregard is sufficient to state a claim for invasion of privacy. Vermont law, however, requires "a substantial, intentional intrusion," *Harris*, 165 Vt. at 439, and Plaintiff offers no controlling authority to support the application of a reckless disregard standard. The motion to dismiss Plaintiff's invasion of privacy claim is therefore granted, and the claim is dismissed without prejudice.

F. Publication of Private Facts

Count Six of the Complaint alleges publication of private facts. PPEC's motion to dismiss properly notes that Vermont has never recognized such a cause of action. Plaintiff's opposition to the motion to dismiss does not offer a meaningful distinction between her publication of private facts claim and her invasion of privacy claim, relying upon the same case law to support both. As discussed previously, those cases are not persuasive. Count Six is therefore dismissed without prejudice.

G. Unjust Enrichment

PPEC moves to dismiss Plaintiff's unjust enrichment claim because Plaintiff has an adequate remedy at law. This District

Court has previously noted that "[a]s an equitable remedy, an unjust enrichment claim lies only when 'there is not an adequate remedy at law on the very subject in question.'" *Ehlers v. Ben & Jerry's Homemade Inc.*, No. 2:19-CV-00194, 2020 WL 2218858, at *9 (D. Vt. May 7, 2020) (quoting *Wynkoop v. Stratthaus*, 2016 VT 5, ¶ 50 (Eaton, J., concurring)); *Moreau v. Sylvester*, 2014 VT 31, ¶ 20). The Complaint expressly acknowledges that the unjust enrichment claim is brought "[i]n the alternative to the above-pleaded claims of breach of contract and breach of implied contractual duty" because, again alternatively, "Plaintiff and the Class allege that they have no adequate remedy at law." ECF No. 1 at 26, ¶ 126.

Such alternative pleading does not require dismissal of the unjust enrichment claim, however, as Federal Rule of Civil Procedure 8(d)(3) allows for pleading in the alternative. *See Doe v. Columbia Univ.*, 831 F.3d 46, 48 (2d Cir. 2016) ("[T]he plaintiff is at liberty to plead different theories, even if they are inconsistent with one another, and the court must accept each sufficiently pleaded theory at face value, without regard to its inconsistency with other parts of the complaint.") (citing Fed. R. Civ. P. 8(d)(3)). The Court must therefore review PPEC's argument as to the sufficiency of the unjust enrichment claim.

To succeed on a claim for unjust enrichment, a "plaintiff must prove that (1) a benefit was conferred on defendant; (2) defendant accepted the benefit; and (3) defendant retained the benefit under such circumstances that it would be inequitable for defendant not to compensate plaintiff for its value." *Center v. Mad River Corp.*, 151 Vt. 408, 412 (1989). PPEC focuses solely on the first element, arguing that the only beneficiary of the private information was its client. As discussed above with respect to the implied-in-fact contract, the Court finds that PPEC shared a benefit with its client. The motion to dismiss the unjust enrichment claim for lack of any benefit to PPEC is therefore denied.

III. Motion to Strike Class Allegations

PPEC's final argument is that the Court should strike the class allegations in the Complaint pursuant to Federal Rule of Civil Procedure 12(f) and find that Plaintiff cannot establish a class under Federal Rule of Civil Procedure 23. Such motions are generally disfavored, as it would require the court "to preemptively terminate the class aspects of litigation, solely on the basis of what is alleged in the complaint, and before plaintiffs are permitted to complete the discovery to which they would otherwise be entitled on questions relevant to class certification." *Ironforge.com v. Paychex, Inc.*, 747 F. Supp. 2d 384, 404 (W.D.N.Y. 2010) (internal citations and quotations

omitted); *Calibuso v. Bank of Am. Corp.*, 893 F. Supp. 2d 374, 383 (E.D.N.Y. 2012) (same). There is an exception to this general rule where the motion to strike addresses issues "separate and apart from the issues that will be decided on a class certification motion." *Rahman v. Smith & Wollensky Rest. Group, Inc.*, 06 Civ. 6198, 2008 WL 161230, at *3 (S.D.N.Y. Jan. 16, 2008).

The exception does not apply here, as PPEC is arguing that the allegations in the Complaint fail to show commonality with respect to the breach victims' injuries. Because commonality is a fundamental requirement for class certification, that issue may be raised by PPEC in the context of a Rule 23 motion. *See Travis v. Navient Corp.*, 460 F. Supp. 3d 269, 286 (E.D.N.Y. 2020) ("Since it would be premature to decide this fact-specific argument at this juncture, [Defendant]'s motion to strike [Plaintiff's] class allegations is denied. [Defendant] may raise these arguments if [Plaintiff] moves for class certification pursuant to Federal Rule of Civil Procedure 23."). The motion to strike is denied.

Conclusion

For the reasons set forth above, PPEC's motion to dismiss (ECF No. 16) is granted in part and denied in part.

DATED at Burlington, in the District of Vermont, this 11th day of October, 2024.

/s/ William K. Sessions III
William K. Sessions III
U.S. District Court Judge